PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Application No.: 09/992,310

Filing Date: November 19, 2001

Applicant: Laurence I. Rockwell

Group Art Unit: 2686

Examiner: Randy Peaches

Title: AIRBORNE SECURITY MANAGER

Attorney Docket: 7784-000188

Director of the United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

DECLARATION UNDER 37 C.F.R. § 1.131

Sir:

I hereby declare under penalty of perjury as follows:

1. That I am the sole inventor of the above-identified application.

2. That the invention was conceived and/or at least partially reduced to practice in this country prior to September 6, 2000, the filing date of the United States Pub. No. 2002/0082886A1 to Manganaris et al.

3. I am the author of the attached presentation whose cover page is attached at Exhibit A. Presentation slides from this presentation are attached as Exhibits B and C and the information contained within Exhibits B and C was prepared by myself.

4. That the invention was conceived and/or reduced to practice prior to September 6, 2000, as evidenced by the presentation slides attached as Exhibits B and C. Exhibits B and C illustrate at least the initial conception and reduction to practice of the invention embodied by at least claim 1.

5. That the invention has never been abandoned, suppressed, or concealed.

6. I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements are being made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, and patent issuing thereon, or any patent to which this verified statement is directed.

Dated: 19 October 2004 Laurence I. Rockwell

Laurence I. Rockwell

Network System Security Architecture

Laurence Rockwell

Items covered in this section:

- Network Security - The problem
- Security Policy
- Key Requirements
- Design Description
- Design Activities / Summary

Focus: Network and Host Based Security, including operational aspects

Not addressed: Environmental Controls (Power Conditioning, UPS, Cooling, Fire detection and suppression), Physical Access Control, Personnel Background, . . .

Connexion by Boeing Security Policy

- Provide (Business) Travelers with onboard (and on ground) network environment as "safe" as when connecting to their ISP from home
- Protect the Connexion Network from:
  - Hackers on the Internet (Connexion will be a high prestige target!)
  - Hackers on the aircraft
  - Hackers on the airwaves
  - Internal unauthorized personnel access
  - Content substitution - e.g. Cyber Graffiti
  - Content Pirating
- Find the appropriate, cost effective balance between functionality and security

Network Security Architectural Principles

Prevention:
- Plug vulnerabilities by hardening hosts
- Use strong passwords / eliminate default passwords
- Implement security enclaves- use firewall technology to deny access to unauthorized personnel
- Use encryption on air links to deny access
- Periodically scan hosts for vulnerabilities
- Implement principle of Least Privilege

Detection: Detect attacks on computing resources
- Host Based
- Network Based

Respond: Close connections or disable interfaces in response to attacks on computing resources

Recovery:
- Minimize downtime through use of controlled media for all software functionality
- Plan and rehearse for contingencies